On Kummer extensions generated by S-units in algebraic number fields

Hiroshi YAMASHITA

Abstract. Let K/k be a Galois extension of algebraic number fields with a Galois group G. Let S be a finite set of places of k containing every archimedian places. Let E_S be the group of S-units of K. We choose a normal subgroup G^* in G and fix it once for all. Denote by k_* the intermediate field corresponding to G^*. Let p be a prime number. We define a subgroup Q_p of E_S to be $\{x \in E_S : x^{p^N} \in k_*\}$ for a sufficiently large integer N. We study the value of a ratio $|Q_p^H : Q_p^H \cap k_*|/[k_*(Q_p^H) : k_*]$. This ratio is a little more subtle to treat when $p = 2$ and $k_* \not\ni \sqrt{-1}$. We need a certain assumption concerning ramification of prime ideals dividing 2 in the subtle case.

1. Introduction. Let k be a finite algebraic number field and K be its finite Galois extension. We choose a normal subgroup G^* of the Galois group $Gal(K/k)$ and fix it once for all. Let k_* be the intermediate field of K/k corresponding to the normal subgroup G^*. When a subgroup H of $Gal(K/k)$ is given, we denote by H^* the subgroup generated by H and G^*, that is $H^* = HG^*$. Let S be a finite set of places of k containing every archimedian places. Denote by $S(K)$ the set of every places of K lying above places belonging to S. Let E_S be the group of $S(K)$-units of K and μ be the torsion subgroup of E_S. We define a subgroup of E_S by

$$Q = \{x \in E_S : x^{|\mu|} \in k_*\}.$$

We note that Q/Q^{G^*} is a finite abelian group and that $Q^H Q^{G^*}/Q^{G^*}$ is isomorphic to Q^H/Q^{H^*} for an arbitrary subgroup H. In the present paper, we shall study the index $|Q^H : Q^{H^*}|$. We define a comparison constant $C(H)$ of the index with the extension degree $[k_*(Q^H) : k_*]$

平成 24 年 9 月 26 日受理

by

$$|Q^H : Q^{H^*}| = C(H)[k_*(Q^H) : k_*].$$

If $k_*(Q^H)/k_*$ is a Kummer extension, it is well-known that $C(H)$ equals one. Hence, our main concern is focused on the case that $k_*(Q^H)$ is not a Kummer extension of k_*.

We proved a formula concerning the Brauer's class number relation in Theorem 9 of [3], where a product

$$\frac{\prod_{H\in\Gamma_0}|Q^H : Q^{H^*}|}{|Q^{G_0} : Q^{G^*}|}$$

of indices $|Q^H : Q^{H^*}|$ for a certain family Γ_0 of subgroups appears. We note that G_0 denotes that the intersection $\cap H$ of subgroups belonging to Γ_0 and that G^* is the normal subgroup defined from Γ_0, which contains G_0. It is inevitable for us to attempt studying the index $|Q^H : Q^{H^*}|$ for each subgroup H. We use classical Kummer theory to this end, especially, the Vahlen-Capelli criterion for reducibility of a polynomial $x^n - a$. According to [1], the criterion is stated as follows:

THEOREM. *Let K be an arbitrary field, $a \in K^\times$ and $n \in \boldsymbol{N}$, $n \geq 2$. Then, $X^n - a$ is reducible in $K[X]$ if and only if either* (i) *there exists $s \in \boldsymbol{N}$, $s > 1$, $s \mid n$ such that $a \in K^s$,* (ii) *$4 \mid n$ and $-4a \in (K^\times)^4$.*

Here, $K^\times$ denotes the multiplicative group of the field, and $(K^\times)^s$ denotes the subgroup consisting of sth power of every element contained in $K^\times$. K^s is union of $(K^\times)^s$ and $\{0\}$. We follow these notations. We notice that the case (ii) is reduced to the case (i) if $\sqrt{-1} \in K$, because $-4a = b^4$ implies $a \in (K^\times)^2$.

In the sequel part, a field is interpreted as a subfield of the field of complex numbers, p denotes a prime number and ζ_{p^n} denotes the complex number $e^{2\pi\sqrt{-1}/p^n}$. Since a finite abelian group is decomposed into a direct sum of the p-primary torsion subgroups, we have

$$Q/Q^{H^*} = \sum_p{}' Q_p/Q^{G^*},$$

where Q_p/Q^{G^*} are p-primary torsion subgroups. Since $Q_p^H Q^{G^*}/Q^{G^*}$ is isomorphic to $Q_p^H/Q_p^{H^*}$ for each p, we obtain

$$Q^H/Q^{H^*} \cong \bigoplus_p Q_p^H/Q_p^{H^*}.$$

We define a constant $C_p(H)$ to be

(1) $|Q_p^H : Q_p^{H^*}| = C_p(H)[k_*(Q_p^H) : k_*]$.

Note $C_p(H) = 1$ except of finite numbers of p's. We study $C_p(H)$'s in place of $C(H)$, because it equals a product of them.

2. An application of the theory of Kummer extensions.

It is obvious that the following lemma holds:

LEMMA 1. *Suppose $x^{p^n} - a$ is irreducible in $k[x]$. Let α be a root of the equation $x^{p^n} - a = 0$. If $k(\alpha)/k$ is a Galois extension, we have $\zeta_p \in k$ and $\zeta_{p^n} \in k(\alpha)$.*

We deal with a subgroup Q' of Q_p^H in general and define a constant $C'_p(H)$ by

(2) $|Q' : k_* \cap Q'| = C'_p(H)[k_*(Q') : k_*]$

Put $k' = k_*(\zeta_{p^N})$ for a sufficiently large integer N and $M = k' \cap k_*(Q')$. We have

(3) $[k_*(Q') : k_*] = [k'(Q') : k'][M : k_*]$.

Since $k'(Q')/k'$ is a Kummer extension whose Kummer group is $Q'(k')^\times/(k')^\times$, we have

(4) $C'_p(H) = |k' \cap Q' : k_* \cap Q'|/[M : k_*]$

from (2) and (3). Let A be the subgroup of $Q_p^H/Q_p^{H^*}$ generated by $k' \cap Q'$. We have

$$A \cong k' \cap Q'/k_* \cap Q'.$$

A is a finite abelian p-group. We see $A \cong \{1\}$ if $M = k_*$.

LEMMA 2. *A is a cyclic group if M/k_* is a cyclic extension.*

Proof. We may assume $M \neq k_*$ and $A \ncong \{1\}$. Let $\overline{\alpha}$ be an element of A with order p. We see $k_*(\alpha)/k_*$ is a cyclic extension of degree p, because $k_*(\alpha)$ is a subfield of M and M/k_* is a cyclic extension. We have $\zeta_p \in k_*$ from Lemma 1, and hence $k_*(\alpha)/k_*$ is a Kummer extension. Since M/k_* is cyclic, every elements of order p contained in A defines the same subfield of M. This implies that there is a unique subgroup of order p in A. Since A is an abelian p-group, it is a cyclic group. □

We lift the extension M/k_* by adjoining ζ_{2p}. Denote by k'_* (*resp.* M') an extension $k_*(\zeta_{2p})$ (*resp.* $M(\zeta_{2p})$). Since M/k_* is an abelian p-extension, we have $M \cap k'_* = k_*$ if $p > 2$. When $p = 2$, we have $M \cap k'_* = k_*$ if and only if $M \ni \sqrt{-1}$ or $k_* \ni \sqrt{-1}$. Let m_0 (*resp.* m) be the maximum of the integers $t \geq 0$ such that $k'_* = k_*(\zeta_{p^t})$ (*resp.* $M' = k_*(\zeta_{p^t})$) holds. We see $m \geq m_0 \geq 1$ and $m_0 \geq 2$ if $p = 2$.

THEOREM 3. *Suppose $\zeta_{2p} \in k_*$. We have A is a cyclic group of order p^{m-m_0} and $C'_p(H) = 1$ if Q' contains ζ_{p^m}.*

Proof. Since $k_* = k'_*$ and $M = M'$, we see M/k_* is a cyclic extension. Thus, we have A is cyclic by Lemma 2. We may assume $m > m_0$. Let $\overline{\zeta_{p^m}}$ be an element of A which ζ_{p^m} generates. Since the order is equal to p^{m-m_0}, we have $p^{m-m_0} = [M : k_*]$ divides $|A|$. Suppose $|A| > p^{m-m_0}$. There is an element $\overline{\alpha}$ in A such that $\overline{\alpha}^p = \overline{\zeta_{p^m}}$ holds. Put $u = \alpha^p \zeta_{p^m}^{-1}$. We have $u \in k_*$ and choose a pth root so that $\alpha = \zeta_{p^{m+1}} \sqrt[p]{u}$ holds. Since α is an element of k', we see $\sqrt[p]{u} \in k'$. However, $\sqrt[p]{u} \notin M$, because of $\zeta_{p^{m+1}} \notin M$. Since k'/k_* is a cyclic extension, we have $k_*(\sqrt[p]{u}) = k_*(\zeta_{p^{m_0+1}})$. This implies $M \ni \sqrt[p]{u}$, because of $\zeta_{p^{m_0+1}} \in M$. We are led into contradiction. Therefore, there is no such $\overline{\alpha}$ in A. Since A is an abelian p-group, it is a cyclic group of order p^{m-m_0} generated by $\overline{\zeta_{p^{m-m_0}}}$. We have $C'_p(H) = 1$ from (4). □

3. Applications of a system of cyclotomic extensions. We concentrate ourselves on the case in which $p = 2$ and

$\sqrt{-1} \notin k_*$. Put $L = k'_* \cap k_*(Q_2^H)$. We have

(5) $[k_*(Q_2^H) : k_*] = [k'_*(Q_2^H) : k'_*][L : k_*]$.

Let B be a subgroup of A generated by $k'_* \cap Q_2^H$:

(6) $B \cong k'_* \cap Q_2^H / k_* \cap Q_2^H$.

We see $B \cong \{1\}$ when $L = k_*$. If $L = k'_*$, B contains an element $\overline{\zeta_4}$ of order two.

LEMMA 4. *We have* $C_2(H) = |B|/2$ *if* $L = k'_*$.

Proof. We see $M' = M$ and $Q_2^H \ni \zeta_{2^m}$ when $L = k'_*$. Let G' be the Galois group of $K/k(\sqrt{-1})$ and put $(G')^* = G' \cap G^*$. $(G')^*$ is a normal subgroup of G' corresponding to k'_*. We have H is a subgroup of G', because $K^H \ni \sqrt{-1}$. Let R be a subgroup of E_S defined for the Galois extension $K/k(\sqrt{-1})$ and the normal subgroup $(G')^*$:

$$R = \{x \in E_S : x^{|\mu|} \in k'_*\}.$$

Let $R_2/R^{(G')^*}$ be the 2-primary torsion subgroup of $R/R^{(G')^*}$. Since Q_2^H is a subgroup of R_2^H containing ζ_{2^m}, we are able to apply Theorem 3 to the case of $Q' = Q_2^H$. We have

$$|Q_2^H : k'_* \cap Q_2^H| = [k'_*(Q_2^H) : k'_*]$$

from (2) and

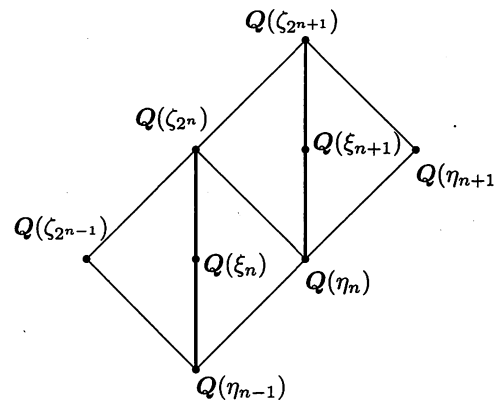
$$|Q_2^H : k_* \cap Q_2^H| = |Q_2^H : k'_* \cap Q_2^H||B|$$

from (6). We obtain

$$|Q_2^H : k_* \cap Q_2^H|/|B| = [k_*(Q_2^H) : k_*]/[L : k_*]$$

from (5). Therefore, $C_2(H) = |B|/2$. □

The cyclotomic extension $\boldsymbol{Q}(\zeta_{2^n})$ contains $\eta_n = \zeta_{2^n} + \zeta_{2^n}^{-1}$ and $\xi_n = \zeta_{2^n} - \zeta_{2^n}^{-1}$. We see $\eta_n^2 = \eta_{n-1} + 2$ and $\xi_n^2 = \eta_{n-1} - 2$. The system of subfields is described by the following Hasse diagram for $n \geq 4$



We define a chain $k_0 \subseteq L_0 \subseteq M_0$ these subfields corresponding to $k \subseteq L \subseteq M$ by

$$k_0 = k_* \cap \boldsymbol{Q}(\zeta_{2^N}) \subseteq L_0 = L \cap \boldsymbol{Q}(\zeta_{2^N}) \subseteq M_0 = M \cap \boldsymbol{Q}(\zeta_{2^N}).$$

Since k_* does not contain $\sqrt{-1}$, we see $k_0 = \boldsymbol{Q}(\eta_{m_0})$ or $k_0 = \boldsymbol{Q}(\xi_{m_0})$. We observe the following four cases may occur:

a) $k_0 = \boldsymbol{Q}(\eta_{m_0})$, $L_0 = \boldsymbol{Q}(\zeta_{2^{m_0}})$, $M_0 = \boldsymbol{Q}(\zeta_{2^m})$.

b) $k_0 = \boldsymbol{Q}(\xi_{m_0})$, $L_0 = \boldsymbol{Q}(\zeta_{2^{m_0}})$, $M_0 = \boldsymbol{Q}(\zeta_{2^m})$.

c) $k_0 = L_0 = \boldsymbol{Q}(\eta_{m_0})$, $M_0 = \boldsymbol{Q}(\eta_m)$.

d) $k_0 = L_0 = \boldsymbol{Q}(\eta_{m_0})$, $M_0 = \boldsymbol{Q}(\xi_m)$.

We notice that L_0 contains $\sqrt{-1}$ if $M \ni \sqrt{-1}$, because L is a subfield of M. L

coincides with k'_* in each case of a) and b). We can prove that B is a cyclic group by a similar argument by which we prove that A is cyclic if M/k_* is a cyclic extension in Lemma 2. Namely, let $\overline{\alpha}$ be an element of B with order 2. $k_*(\alpha)$ is a quadratic extension and is contained in k'_*. Thus, $k_*(\alpha) = L$. This implies $\alpha \in \sqrt{-1}(k_*^\times)$ by Kummer theory, because of $L = k_*(\sqrt{-1})$. Therefore, we have there is a unique element of order 2 in B. It follows that B is cyclic.

Let S_2 be the set of every places of k lying above 2.

LEMMA 5. *B is a cyclic group generated by $\overline{\zeta_{2^{m_0}}}$ in the case of b).*

Proof. We prove B is cyclic in the above. Suppose there is $\overline{\alpha} \in B$ such that $\overline{\alpha}^2 = \overline{\zeta_{2^{m_0}}}$. We have $u = \alpha^2\zeta_{2^{m_0}}^{-1}$ is contained in k_* and choose an element $\sqrt{u}$ of k' so that $\alpha = \zeta_{2^{m_0+1}}\sqrt{u}$ holds. We observe that $\boldsymbol{Q}(\zeta_{2^N})/k_0$ is a cyclic extension in the above Hasse diagram. Since $k_*(\sqrt{-1}, \sqrt{u})$ is a subfield of k', we have $k_*(\sqrt{-1}, \sqrt{u})$ is also cyclic over k_*. Thus, there is $x \in k_*$ such that $\sqrt{u} = \sqrt{-1}x$ holds. However, since $\alpha = \zeta_{2^{m_0+1}}(\sqrt{-1}x) \in L$, we obtain $\zeta_{2^{m_0+1}} \in L$. This contradicts the definition of the number m_0. There is no such α in B. Hence, B is a cyclic group generated by $\overline{\zeta_{2^{m_0}}}$. □

We observe $\boldsymbol{Q}(\zeta_{2^{m_0+1}})$ coincides with $\boldsymbol{Q}(\zeta_{2^{m_0}}, \eta_{m_0+1})$ from the Hasse diagram. We see $\boldsymbol{Q}(\zeta_{2^{m_0+1}})$ is a quadratic extension over $\boldsymbol{Q}(\zeta_{2^{m_0}})$ generated by $\zeta_{2^{m_0+1}}$ or η_{m_0+1}. Hence, $\rho_{m_0} = \zeta_{2^{m_0+1}}\eta_{m_0+1}$ is an element of $\boldsymbol{Q}(\zeta_{2^{m_0}})$. We have $\rho_{m_0}^{2^t} \in \boldsymbol{Q}(\eta_{2^{m_0}})$ if and only if $t \equiv 0 \mod m_0$.

LEMMA 6. *We suppose in the case of a) that every prime divisors dividing 2 in k_* have odd ramification indices over $k_0 = \boldsymbol{Q}(\eta_{m_0})$. Then, we have B is a cyclic group. Moreover, B is generated by $\overline{\rho_{m_0}}$ if $S \supset S_2$ and does by $\overline{\zeta_{2^{m_0}}}$ if $S \not\supset S_2$.*

Proof. Let $\mathfrak{p}_{m_0}$ be the prime ideal dividing 2 in k_0. We note that $\mathfrak{p}_{m_0}$ is a principal ideal generated by $\eta_{m_0+1}^2 = \eta_{m_0} + 2$ or $\xi_{m_0+1}^2 = \eta_{m_0} - 2$. Let

$$\mathfrak{p}_{m_0} = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r} \tag{7}$$

be the factorization of $\mathfrak{p}_{m_0}$ to prime ideals in k_*.

When $S \supset S_2$, we see $\rho_{m_0} \in Q_2^H$. Suppose there is $\overline{\alpha}$ in B such that $\overline{\alpha}^2 = \overline{\rho_{m_0}}$ holds. We have $u = \alpha^2\rho_{m_0}^{-1}$ is an element of k_*. We choose a square root so that

$$\alpha = \sqrt{\zeta_{2^{m_0+1}}}\sqrt{\eta_{m_0+1}u} \tag{8}$$

holds. Put $\theta = \sqrt{\eta_{m_0+1}u}$. We see $\theta \in k'$, because α and $\sqrt{\zeta_{2^{m_0+1}}}$ belong to k'. If θ is an element of $k_*(\eta_{m_0+1})$, we have $x \in k_*(\eta_{m_0+1})$ such that $\eta_{m_0+1}u = x^2$ holds. Thus, we obtain $\mathfrak{p}_{m_0}(u^2) = (x^4)$ in $k_*(\eta_{m_0+1})$. Since $k_*(\eta_{m_0+1})/k_*$ is a quadratic extension, we see that

the ideal (x) is invariant by action of $Gal(k_*(\eta_{m_0+1})/k_*)$ and that (x^2) is a natural extension of an ideal of k_*. Hence, $\mathfrak{p}_{m_0}$ is a square of an ideal in k_*. This implies every e_i's in (7) are even. Therefore, if one of e_i's is odd, we have $\theta \notin k_*(\eta_{m_0+1})$. Thus, $k_*(\theta)$ is a quadratic extension of $k_*(\eta_{m_0+1})$ and is a quartic extension over k_*. This implies $x^4 - \theta^4$ is irreducible over k_*. Since $\theta \in k'$, we have $k_*(\theta)/k_*$ is an abelian extension. It follows from Lemma 1 that $k_*(\theta)$ contains $\sqrt{-1}$. Since $k_*(\sqrt{-1}, \eta_{m_0+1})$ is also quartic over k_*, we have $k_*(\theta) = k_*(\sqrt{-1}, \eta_{m_0+1}) = k_*(\zeta_{2^{m_0+1}})$. However, since $\alpha \in L = k_*(\zeta_{2^{m_0}})$ and since $\sqrt{\zeta_{m_0+1}} = \alpha\theta^{-1}$ from (8), $k_*(\zeta_{2^{m_0+1}})$ must contain $\zeta_{2^{m_0+2}}$. We are led into contradiction. Therefore, there is no $\overline{\alpha}$ in B such that $\overline{\alpha}^2 = \overline{\rho_{m_0}}$ holds. B is a cyclic group generated by $\overline{\rho_{m_0}}$

We suppose there is $\overline{\alpha}$ in B such that $\overline{\alpha}^2 = \overline{\zeta_{2^{m_0}}}$ holds when S does not contain S_2. $u = \alpha^2\zeta_{2^{m_0}}^{-1}$ is an element of k_* and there is $\sqrt{u}$ satisfying $\alpha = \zeta_{2^{m_0+1}}\sqrt{u}$. We see $\sqrt{u} \in k'$, $\sqrt{u} \notin k_*(\sqrt{-1})$, because of $\alpha \in k_*(\sqrt{-1})$ and $\zeta_{2^{m_0+1}} \notin k_*(\sqrt{-1})$. Hence, $k_*(\sqrt{-1}, \sqrt{u})$ is a biquadratic extension of k_* contained in k'. Since $\boldsymbol{Q}(\zeta_{2^{m_0+1}})/k_0$ is a biquadratic extension, we have $k_*(\zeta_{2^{m_0+1}})/k_*$ is also biquadratic. Thus, $k_*(\sqrt{-1}, \sqrt{u}) = k_*(\zeta_{2^{m_0+1}})$. We observe $k_*(\zeta_{2^{m_0+1}}) = k_*(\sqrt{-1}, \eta_{m_0+1}) = k_*(\sqrt{-1}, \xi_{m_0+1})$. This implies $\sqrt{u}\eta_{m_0+1}^{-1} \in k_*$ or $\sqrt{u}\xi_{m_0+1}^{-1} \in k_*$ by Kummer theory, because of $\eta_{m_0+}\xi_{m_0+1} = \xi_{m_0} \notin k_*$. If $x = \sqrt{u}\eta_{m_0+1}^{-1} \in k_*$ (*resp.* $y = \sqrt{u}\eta_{m_0+1}^{-1} \in k_*$), we have $\mathfrak{p}_{m_0} = (ux^{-2})$ (*resp.* $\mathfrak{p}_{m_0} = (uy^{-2})$). Let $\mathfrak{P}_i$ be a prime divisor in k_* dividing 2 such that $\mathfrak{P}_i \nmid u$. The exponent e_i of the prime divisor in (7) must be even. This is impossible. Therefore, there is no $\overline{\alpha}$ in B such that $\overline{\alpha}^2 = \overline{\zeta_{2^{m_0}}}$ holds. B is a cyclic group generated by $\overline{\zeta_{2^{m_0}}}$. □

By Lemma 4, 5 and 6, we obtain

THEOREM 7. *We have $C_2(H) = 2^{m_0-2}$ in the case b). If every prime ideals of k_* dividing 2 have odd ramification indices over k_0, we have in the case a) that $C_2(H)$ equals 2^{m_0-1} when $S \supset S_2$, and equals 2^{m_0-2} when $S \not\supset S_2$.*

REMARK 1. Set $k = \boldsymbol{Q}(\eta_{m_0+1})$ and $K = k(\zeta_{2^{m_0+1}}, \sqrt{\rho_{m_0}})$. Let σ be restriction onto K of the complex conjugation map. σ generates the Galois group of $k(\zeta_{2^{m_0+1}})/k$ and $\rho_{m_0}^{\sigma} = \zeta_{2^{m_0+1}}^{-2}\rho_{m_0}$. Therefore, K/k is a Galois extension. Set $G^* = Gal(K/k)$ and S to union of the set consisting of every archimedian places and a set $\{\mathfrak{p}_{m_0}\}$. Put $H = \{id_K\}$. We see $k_* = k$, $L = k(\zeta_{2^{m_0+1}})$ and $\sqrt{\rho_{m_0}} \in Q_2^H$. Then, $\overline{\sqrt{\rho_{m_0}}}$ is an element of order 2^{m_0+1} in B.

THEOREM 8. *We have $2^{m_0-m} \leq C_2(H) \leq 2^{m_0-m+1}$ in cases c) and d).*

Proof. Since $k' = k_*(\zeta_{2^N})$ and $k' \supset M$, we have $M_0 k_* = M$. We observe that $\sqrt{-1}$ is not contained in M and that M/k_* is a cyclic extension of degree 2^{m-m_0}. If $m = m_0$, we see $|A| = 1$ and $C_2(H) = 1$. Let $\overline{\alpha}$ be an element of order 2^n in A. Suppose $n > 1$ when $m > m_0$. We have $k_*(\alpha)$ is an abelian extension of k_*, because it is a subfield of M. If $x^{2^n} - \alpha^{2^n}$ is irreducible over k_*, we obtain $k_*(\alpha) \ni \sqrt{-1}$ by Lemma 1. However, this is not the case. If $x^{2^n} - \alpha^{2^n}$ is reducible, we have $-4\alpha^{2^n} = b^4$ holds for $b \in k_*^\times$ by the Vahlen-Capelli criterion, we also have $\sqrt{-1} \in k_*$. This is not possible. Hence, there is no such $\overline{\alpha}$ in A. This proves every element of A have order less than 4. Since A is a cyclic group by Lemma 2, we see $|A| \leq 2$. The assertion follows from the formula (4). □

4. Degree of a Kummer extension. Let μ_* be the maximal p-primary torsion subgroup of $k_*^\times$. Let p^s be the order. We have $s = m_0$ if k_* contains ζ_{2p}. Let x be an element of k_* which is not contained in $k_*^p \cup \mu_*$. There is a unique integer $n_0 \geq 0$ satisfying

$$x^{p^s} \in (k_*)^{p^{n_0+s}} - (k_*)^{p^{n_0+s+1}}. \tag{9}$$

We solve the equation $x^{p^s} = y^{p^{n_0+s}}$, $y \in k_*$ and obtain $\zeta \in \mu_*$ such that $x = \zeta y^{p^{n_0}}$ holds. We note $\zeta \notin \mu_*^p$ if $n_0 > 0$. If there is another expression $x = \zeta_1 y_1^{p^{n_1}}$ for $\zeta_1 \in \mu_*$ and $n_1 \geq 0$, we see $y^{p^{n_0+s}} = y_1^{p^{n_1+s}}$. It follows from (9) that n_1 is not greater than n_0. We have $\zeta' = y_1 y^{-1} \in \mu_*$ and $\zeta = \zeta_1 \zeta'^{p^{n_0}}$ if $n_0 = n_1$. Hence, the order of ζ is uniquely determined if $n_0 > 0$. Based on these observations, we classify elements α of $Q_p^H - k_* \cup \mu_* \cup Q_p^{H^*}$ into the following three types:

(i) $\alpha^{p^n} = a, a^{p^s} \notin k_*^{p^{s+1}}, n_0 = 0.$

(ii) $\alpha^{p^n} = \zeta_{p^s}^h a^{p^{n_0}}, a^{p^s} \notin k_*^{p^{s+1}}, n > n_0 > 0.$

(iii) $\alpha^{p^n} = \zeta_{p^s}^h a^{p^{n_0}}, a^{p^s} \notin k_*^{p^{s+1}}, 0 < n \leq n_0.$

We note that the order of $\overline{\alpha}$ in $Q_p^H/Q_p^{H^*}$ is p^n, h is prime to p and that $k_*(\alpha)$ is a subfield of k' if α is of the type (iii). We call α is regular if it is of the type (i) or of the type (ii). If α is of the type (ii), there are integers h_1 and h_2 which are not divided by p and satisfy

$$\alpha^{p^{n-n_0}} = \zeta_{p^{s+n_0}}^{h_1} a, \tag{10}$$

$$\alpha^{p^{n-n_0-1}} = \zeta_{p^{s+n_0+1}}^{h_2} \sqrt[p]{a}, \tag{11}$$

where $\sqrt[p]{a}$ is a solution of $x^p - a$. Since k'/k_* is a Galois extension, $\sqrt[p]{a} \notin k'$ is equivalent to that $x^p - a$ has no solution in k'.

LEMMA 9. *Let α be a regular element. We have $\sqrt[p]{a} \notin k'$ if $\zeta_{2p} \in k_*$, or if $p = 2$, $\sqrt{-1} \notin k_*$ and $a \notin (\eta_{m_0} \pm 2)(k_*^\times)^2$.*

Proof. When $\zeta_{2p} \in k_*$, we have $k_* = k_*(\zeta_{p^{m_0}})$ and k'/k_* is a cyclic extension. Since $k_*(\sqrt[p]{a})$ is of degree p over k_*, we have $k_*(\sqrt[p]{a}) = k_*(\zeta_{2^{m_0+1}})$ if $\sqrt[p]{a} \in k'$.

Thereat, there is an integer j and $b \in k_*$ such that $p \nmid j$ and such that $\sqrt[p]{a} = \zeta_{p^{m_0+1}}^{j} b$. This implies $a^{p^{m_0}} = b^{p^{m_0+1}}$. Since $s = m_0$, this is not true. Therefore, we have $\sqrt[p]{a} \notin k'$.

When $p = 2$ and $\sqrt{-1} \notin k_*$, we have $b \in k_*$ such that $\sqrt{a} = \sqrt{-1}b$ holds if $k'_* = k_*(\sqrt{a})$. This is also not true. Hence, we have $k'_* \neq k_*(\sqrt{a})$ and $k_*(\sqrt{-1}, \sqrt{a})$ is a biquadratic extension of k_*. If $\sqrt{a} \in k'$, the biquadratic extension is a subfield of k'. Since k'/k_* is not cyclic, we have $k_0 = \boldsymbol{Q}(\eta_{m_0})$. We observe from the Hasse diagram that $\boldsymbol{Q}(\zeta_{2^{m_0+1}})$ is a biquadratic extension over k_0. It follows $k_*(\sqrt{-1}, \sqrt{a}) = k_*(\zeta_{2^{m_0+1}})$. Since $k_*(\zeta_{2^{m_0+1}})$ is generated by $\sqrt{-1}$ and η_{m_0+1} or by $\sqrt{-1}$ and ξ_{m_0+1}, we have $\sqrt{a}\eta_{m_0+1}^{-1}$ or $\sqrt{a}\xi_{m_0+1}^{-1}$ is an element of k_*. This implies $a \in (\eta_{m_0} + 2)(k_*^{\times})^2$ or $a \in (\eta_{m_0} - 2)(k_*^{\times})^2$. Therefore, if $a \notin (\eta_{m_0} \pm 2)(k_*^{\times})^2$, we have $\sqrt{a} \notin k'$. □

PROPOSITION 10. *Let α be a regular element. We have $[k'(\alpha) : k'] = p^{n-n_0}$ if $\sqrt{a} \notin k'$.*

Proof. Let $\sqrt[p]{\alpha}$ be a solution of the equation $x^p - a = 0$ in $k(\alpha)$ and j be an integer such that $\alpha^{p^{n-n_0-1}} = \zeta_{p^{s+n_0+1}}^{j} \sqrt[p]{a}$ holds. If α is of type (i), we may choose $j = p^{s+1}$. We have $\alpha^{p^{n-n_0}} \in k'$ and $\alpha^{p^{n-n_0-1}} \notin k'$, because of $\sqrt[p]{a} \notin k'$. By Vahlen-Capelli criterion, $x^{p^{n-n_0}} - \alpha^{p^{n-n_0}}$ is irreducible over k'. We have $[k'(\alpha) : k'] = p^{n-n_0}$. □

We set Q' to a subgroup of Q_p^H generated by a regular element α in the formula (2). Suppose $\sqrt[p]{a} \notin k'$. We have $\beta = \alpha^{p^{n-n_0}}$ is an element of $k' \cap Q'$ and $\overline{\beta}$ generates A. Hence, $|A| = p^{n_0}$. It follows from (4) that

(12) $\quad C'_p(H) = p^{n_0}/[M : k_*]$,

holds, where $M = k' \cap k_*(\alpha)$, which coincides with $k_*(\alpha^{p^{n-n_0}})$. We have $C'_p(H) = 1$ if and only if $x^{p^{n_0}} - \alpha^{p^n}$ is irreducible over k_*. If $\zeta_{2p} \in k_*$ or if α is of type (i), the equation is irreducible. If $p = 2$, $\sqrt{-1} \notin k_*$ and if α is of type (ii), we observe that $x^2 - \alpha^{2^n}$ is irreducible and that $x^{2^{n_0}} - \alpha^{2^n}$ for $n_0 \geq 2$ is reducible by the Vahlen-Capelli criterion if and only if there is $b \in k_*$ such that $4a^{2^{n_0}} = b^4$ holds. Hence, $x^{2^{n_0}} - \alpha^{2^n}$ is irreducible for $n_0 \geq 2$ if and only if $\sqrt{\pm 2} \notin k_*$.

REMARK 2. Let m_0 be an integer greater than 2. Set K to a Galois extension $\boldsymbol{Q}(\zeta_{2^{m_0(m_0-1)}}, \sqrt[2^{m_0}]{\eta_{m_0}})$ over $k = \boldsymbol{Q}(\eta_{m_0})$. Let σ be an automorphism of $\boldsymbol{Q}(\zeta_{2^N})$ defined by $\zeta_{2^N}^{\sigma} = \zeta_{2^N}^{1+2^{m_0-1}}$. We see $\eta_{m_0}^{\sigma} = -\eta_{m_0}$. Hence, $\sqrt{\eta_{m_0}}^{\sigma}$ is not real and $\sqrt{\eta_{m_0}}$ is real. Since $\boldsymbol{Q}(\zeta_{2^N})$ is a CM-field, we have $\sqrt{\eta_{m_0}} \notin \boldsymbol{Q}(\zeta_{2^N})$. Therefore, $\sqrt{\eta_{m_0}} \notin \boldsymbol{Q}(\zeta_{2^N})$. Suppose $S \supset S_2$. $\alpha = \sqrt[2^{m_0}]{\rho_{m_0-1}}$ is an element of Q_2 such that $\alpha^{2^{m_0(m_0-1)}} = -\eta_{m_0}^{2^{m_0-1}}$ and $\eta_{m_0}^2 \notin k^4$. Put $G_* = G$, $H = Gal(K/k(\alpha))$. We see $M = k_*(\zeta_{2^{m_0}})$ from (11). Hence, $C'_2(H) = 2^{m_0-2}$ from the formula (12). We note $\sqrt{2} \in \boldsymbol{Q}(\eta_{m_0})$.

5. Posets of subfields. The set consisting of every intermediates fields of $k_*(\alpha)/k_*$ is a set equipped with partial order which inclusion defines. The structure of this poset influences the value of $C'_p(H)$ when Q' is a subgroup of Q_p^H generated by α. We study its structure in this section. Denote by I_{L/k_*} the poset of intermediate fields for an extension L/k_*.

PROPOSITION 11. *Suppose $\zeta_{2p} \in k_*$ and $x^{p^n} - a$ is irreducible over k_*. Let α be a root of $x^{p^n} - a$. Then, we have $I_{k_*(\alpha)/k_*} = \{k_*(\alpha^{p^i}) : 0 \leq i \leq n\}$, which is totally ordered set.*

Proof. By the Vahlen-Capelli criterion, $x^{p^{n-i}} - a$ is irreducible for each $0 \leq i \leq n$. Hence, $[k_*(\alpha^{p^i}) : k_*] = p^{n-i}$. This implies $k_*(\alpha^i) \neq k_*(\alpha^j)$ if $i \neq j$. The assertion is obvious when $n = 1$. We prove by induction. Let $n \geq 2$. Suppose there is a maximal intermediate field M in $k_*(\alpha)/k_*$ which is different from $k_*(\alpha^p)$. We see $L = M \cap k_*(\alpha^p)$ is a proper subfield of $k_*(\alpha^p)$. Hence, we have $L = k_*(\alpha^m)$ for $m \geq 2$ by hypothesis of induction. Let t_0 be the minimum of integers $t \geq 0$ such that $\alpha^{p^t} \in M$. We see $2 \leq t_0 \leq m$ and $\alpha^{p^{t_0}} \in M \cap k_*(\alpha^{p^2}) \subset L$. Thus, $[k_*(\alpha^{p^{t_0}}) : k_*] \leq [k_*(\alpha^{p^m}) : k_*]$. We have $t_0 \geq m$. Therefore, $t_0 = m$. If $x^{p^m} - \alpha^{p^m}$ is irreducible over M, we have $p^m = [k_*(\alpha) : M] \leq [k_*(\alpha) : L] \leq p^m$. This implies $M = L$. This is not the case. Hence, $x^{p^m} - \alpha^{p^m}$ must be reducible over M. By the Vahlen-Capelli criterion, there is $y \in M$ such that $\alpha^{p^m} = y^p$. We have $\alpha^{p^{m-1}}$ belongs to M, because of $\zeta_p \in M$. This contradicts the definition of the number m. We conclude that the maximal subfield M dose not exists in $k_*(\alpha)$. Therefore, an intermediate field of $k_*(\alpha)/k_*$ is a subfield of $k_*(\alpha^p)$ if it does not coincide with $k_*(\alpha)$. This proves the proposition. □

Now, we assume $p = 2$ and $k_* \ni \sqrt{-1}$. Let α be an element such that

(13) $\alpha^{2^n} = -a^{2^{n_0}}, a^2 \notin k_*^4, n > n_0 \geq 1.$

We see $k_*(\alpha) \ni \sqrt{-1}$. Let l be the minimum of integers $t \geq 0$ such that $\alpha^{2^t} \in k'_* = k_*(\sqrt{-1})$ holds. Since $\alpha^{2^{l-1}} \notin k'_*$, we have $x^{2^l} - \alpha^{2^l}$ is irreducible over k'_* by the Vahlen-Capelli criterion. Hence, $k_*(\alpha)$ is of degree 2^l over k'_*. Let M be a maximal intermediate field of $k_*(\alpha)/k_*$ which does not contain $\sqrt{-1}$. By virtue of Proposition 11, we have an integer m such that $0 \leq m \leq l$ and $M(\sqrt{-1}) = k'_*(\alpha^{2^{l-m}})$ hold. Put $K_i = k'_*(\alpha^{2^{l-i}})$ and $M_i = K_i \cap M$ for $0 \leq i \leq m$. We see $M_m = M$, $M_0 = k_*$ and $K_m = M_m(\sqrt{-1})$. Since $M_i(\sqrt{-1})$ is a quadratic extension of M_i contained in K_i, we have $[K_i : M_i] \geq 2$. Put $\alpha_0 = \alpha^{2^{l-m}}$. There is a conjugate element β_0 over M of α_0 in $k'_*(\alpha_0)$. We notice that $\beta_0^{2^m}$ belongs to k'_*, because k'_* is a Galois extension of k_* and $\alpha_0^{2^m}$ is an

element of k'_*. Hence, $x^{2^i} - \beta_0^{2^m}$ is conjugate to $x^{2^i} - \alpha_0^{2^m}$ over k_*. We have $[k'_*(\beta_0^{2^{m-i}}) : k'_*] = 2^i$ from irreducibility of $x^{2^i} - \alpha_0^{2^m}$. It follows from Proposition 11 that $k'_*(\beta_0^{2^{m-i}})$ is consistent with $k'_*(\alpha_0^{2^{m-i}})$. Set $\gamma_i = \alpha_0^{2^{m-i}} + \beta_0^{2^{m-i}}$ and $\delta_i = (\alpha_0\beta_0)^{2^{m-i}}$. We have $\gamma_i, \delta_i \in M_i$, because γ_i and δ_i belong to M. Since $\alpha_0^{2^{m-i}}$ is a root of a quadratic equation $x^2 - \gamma_i x + \delta_i = 0$, we obtain $[K_i : M_i] \leq 2$, and hence K_i/M_i is a quadratic extension.

PROPOSITION 12. *I_{M/k_*} is totally ordered.*

Proof. We have $[M_i : M_{i-1}] = 2$, because

$$[K_i : M_{i-1}] = [K_i : M_i][M_i : M_{i-1}] = [K_i : K_{i-1}][K_{i-1} : M_{i-1}]$$

holds. Suppose there is a maximal intermediate field M' in M_i/k_* which is different from M_{i-1}. We see $M'(\sqrt{-1}) \subseteq K_i$. Since the poset $I_{k_*(\alpha)/k'_*}$ is totally ordered by Proposition 11, $M'(\sqrt{-1})$ must be contained in K_{i-1} if $M'(\sqrt{-1}) \neq K_i$. Furthermore, $M' \subseteq M_{i-1}$ follows from $M'(\sqrt{-1}) \subseteq K_{i-1}$. This is not true. We have $M'(\sqrt{-1}) = K_i$. Nevertheless, there exists the following contradiction:

$$[K_i : M'] = [K_i : M_i][M_i : M'] \geq 4,$$
$$[K_i : M'] = [M'(\sqrt{-1}) : M'] = 2.$$

Therefore, such maximal intermediate field M' does not exist. M_{i-1} is a unique maximal intermediate field of M_i/k_*. This proves I_{M/k_*} is totally ordered, □

When α is of the type (i) for $p = 2$, we have $\sqrt{-1} \notin k_*(\sqrt{a})$. If $x^{2^n} - a$ is reducible over $k'_* = k_*(\sqrt{-1})$, there is $\beta \in k'_*$ such that $\beta^2 = a$. Since $\beta \in K_*(\sqrt{a})$, we obtain $k_*(\beta) \subseteq k'_* \cap k_*(\sqrt{a})$. Hence, $\beta \in k_*$. This implies that α is not of the type (i). We conclude $x^{2^n} - a$ is irreducible over k'_*. Let M be an intermediate field of $k_*(\alpha)/k_*$. By Proposition 11, there is an integer m such that $0 \leq m \leq n$ and $M(\sqrt{-1}) = k'_*(\alpha^{2^m})$. Let σ be a generator of the Galois group of $k'_*(\alpha)/k_*(\alpha)$. σ also generates $Gal(M(\sqrt{-1})/M)$ and $Gal(k'_*(\alpha^{2^m})/k_*(\alpha^{2^m}))$. Hence, $M = k_*(\alpha^{2^m})$. We notice that there is a bijection between $I_{k'_*(\alpha)/k'_*}$ and $I_{k_*(\alpha)/k_*}$. Therefore, we have $I_{k_*(\alpha)/k_*} = \{k_*(\alpha^{2^i}) : 0 \leq i \leq n\}$.

References

[1] T. ALBU; Kummer extensions with few roots of unity. J. of Number Th. **41**(1992), 322–358.

[2] C. WALTER; Kuroda's class number relation. Acta Arith. **35**(1979), 41–51.

[3] H. YAMASHITA; A note on the index formula of the group of S-units concerning Brauer's class number relation. Bull. of the School of Teacher Edu., College of Human and Social Sci., Kanazawa Univ. **No.3**(2011), 31–41.